Blockchain Security Monthly Recap of July: $415M lost in attacks

It's time for our monthly security review! According to the data from Beosin EagleEye, various types of security incidents and losses in July 2023 have significantly increased compared to June. There were over 31 typical security events in July, with a total loss of ＄415 million. Among them, the total amount of losses from attack incidents was approximately $180 million, a significant increase of 89% from June, and the total amount of Rug Pull incidents was $24.46 million, about five times that of June. Additionally, the MultiChain abnormal fund flow incident involved $210 million.

In July, there were several security incidents with losses exceeding tens of millions of dollars: MultiChain experienced an abnormal fund outflow of $210 million ; Old versions of Vyper caused multiple Curve pool attacks, resulting in a loss of $61.7 million; Alphapo's hot wallet was hacked, leading to a loss of $60 million; The crypto payment service provider CoinsPaid suffered a theft of $37.3 million; The cross-chain protocol Poly Network was attacked, resulting in a loss of $10.1 million; Additionally, there were numerous scam and rug pull events in July, with the largest amount involved in the BALD project on the Base chain, where the deployer made a profit of approximately $9.28 million.

DeFi

『17』Typical Security Incidents

No. 1 On July 2nd, the Aave fork project on the Pulse chain suffered a governance attack, resulting in a loss of approximately $900,000.
No. 2 On July 2nd, the cross-chain protocol Poly Network suffered an attack, suspected to be caused by private key leakage, leading to a loss of approximately $10.1 million.
No.3 Starting from July 7th, a total of $ 210 millionwas drained from the Multichain bridge. On July 14th, according to an official tweet, the funds were transferred by the team CEO's family, and CEO Zhao Jun was taken away by the Chinese police, leading to the forced suspension of Multichain's operations.
No.4 On July 8th, the Civfund contract was attacked, resulting in a loss of approximately $180,000.
No.5 On July 10th, ArcadiaFi was attacked on both the Ethereum and Optimism chains, leading to a loss of approximately $450,000.
No.6 On July 11th, Libertify was attacked for reentrancy on the Polygon and Ethereum chains, leading to a loss of approximately $450,000.
No.7 On July 11th, the Rodeo Finance leverage revenue protocol in the Arbitrum ecosystem was attacked for price manipulation, leading to a loss of approximately $880,000.
No.8 On July 12th, WGPT on the BNB chain was attacked in a flash loan attack, resulting in a loss of approximately $80,000.
No.9 On July 18th, BNO on the BNB chain was attacked in a flash loan attack, resulting in a loss of approximately $500,000.
No.10 On July 20th, a series of airdrop() vulnerability attacks occurred on the BNB chain, involving multiple tokens such as FFIST, AI-Doge, QX, and Utopia, resulting in a total loss of approximately $300,000.
No.11 On July 21st, Conic Finance was attacked for reentrancy, resulting in a loss of approximately $3.2 million.
No.12 On July 22nd, the Estonian encrypted payment service provider CoinsPaid reported an attack, with $37.3 million worth of cryptocurrencies stolen.
No.13 On July 25th, Palmswap on the BNB chain was attacked, resulting in a loss of approximately $900,000.
No.14 On July 25th, the lending protocol Eralend on Zksync was attacked in a flash loan attack, resulting in a loss of approximately $3.4 million.
No.15 The hot wallet of the cryptocurrency payment service provider Alphapo was hacked, resulting in a loss of $60 million.
No.16 On July 27th, Carson on the BNB chain was attacked, resulting in a loss of approximately $140,000.
No.17 On July 30th, multiple Curve pools were attacked by hackers due to the failure of the anti-reentrancy lock in the old versions of Vyper (0.2.15, 0.2.16, and 0.3.0), resulting

in a total loss of $61.7 million for the pETH/ETH, msETH/ETH, alETH/ETH, and CRV/ETH pools.

Rug Pull/Crypto Scam

『8』Typical Security Incidents

No.1 On July 3rd, a crypto project called Encryption AI experienced a rug pull, with developers making off with $2 million and posting a notice on social media claiming to be "seriously addicted to gambling."
No.2 On July 18th, GMETA on the BSC suffered a rug pull, with the deployer making a profit of $3.67 million.
No.3 On July 19th, IPO token on the BSC experienced a rug pull, with the deployer making a profit of $480,000.
No.4 On July 20th, the Flashmall project on BSC experienced a rug pull, with the deployer making a profit of $550,000.
No.5 On July 22nd, IEGT token on the BSC experienced a rug pull, with the deployer making a profit of approximately $1.14 million.
No.6 On July 28th, DefiLabs on the BNB chain pulled a scam and ran away, with scammers making a profit of $1.4 million. DefiLabs claimed on Twitter that they encountered unexpected issues during "maintenance and updates."
No.7 On July 29th, the zkSync Era yield aggregator protocol, Kannagi Finance, experienced a Rug Pull event, involving an amount of approximately $2.13 million.
No.8 On July 31st, the Base chain project BALD suffered a Rug Pull, with the deployer profiting around 5000 ETH (approximately $9.28 million).

Crypto Crime/Regulatory Cases

『6』Typical Security Incidents

No.1 On July 11th, the U.S. Department of Justice announced the first criminal case involving a smart contract attack on DEX. Shakeeb Ahmed, a senior security engineer at an international tech company, used his expertise to defraud exchanges and their users, stealing approximately $9 million worth of cryptocurrencies.
No.2 On July 18th, the Hubei police in China cracked the country's first case involving virtual currencies, involving transactions amounting to 400 billion RMB.

No.3 On July 18th, Eddy Alexandr, the founder of the New York encrypted trading platform EminiFX, was sentenced to nine years in prison for defrauding over 25,000 investors on the EminiFX platform, with a total amount exceeding $248 million.
No.4 On July 25th, the U.S. Commodity Futures Trading Commission (CFTC) charged Michael and Amanda Griffis from Tennessee, accusing them of defrauding over 100 people through a digital asset commodity pool named "Blessings of God Thru Crypto," raising over $6 million.
No.5 On July 25th, South Korean prosecutors filed charges against 49 individuals suspected of engaging in virtual asset speculation. They allegedly gained 390 billion Korean won (approximately $304 million) in improper profits through virtual asset speculation.
No.6 On July 28th, a UK court sentenced two cryptocurrency scammers to six years in prison. The case involved an amount of approximately 500,000 pounds (approximately $661,000).

Given the current security situation, Beosin presents the following summary for July 2023:
Overall, there has been a significant increase in the number of various blockchain security incidents and the total amount of losses reached $415 million.

The incidents involving PolyNetwork, Alphapo, and other private key leaks resulted in substantial losses. Therefore, it is highly recommended for project teams to establish strict private key management processes, implement multi-signature mechanisms, and avoid using private keys in internet-connected environments. Additionally, the occurrence of reentrancy attacks saw a considerable rise this month. To address this issue, it is advisable for project teams to seek professional security companies for auditing before project going live. Furthermore, the Vyper compiler version vulnerability that emerged this month requires efforts from the community to propose improvement solutions. Lastly, there has been a notable increase in Rug Pull events this month. Users are advised to conduct thorough background investigations on projects and review relevant audit reports to avoid asset losses.

Beosin is a leading global blockchain security company co-founded by several professors from world-renowned universities and there are 40+ PhDs in the team, and set up offices in 10+ cities including Hong Kong, Singapore, Tokyo and Miami. With the mission of "Securing Blockchain Ecosystem", Beosin provides "All-in-one" blockchain security solution covering Smart Contract Audit, Risk Monitoring & Alert, KYT/AML, and Crypto Tracing. Beosin has already audited more than 3000 smart contracts including famous Web3 projects PancakeSwap, Uniswap, DAI, OKSwap and all of them are monitored by Beosin EagleEye. The KYT AML are serving 100+ institutions including Binance.